LevelBlue

CASE STUDY

LevelBlue assists municipality hit by ransomware attack

A large local government entity suffered a ransomware attack. This case study discusses LevelBlue's rapid investigation of the attack and support in helping the client to recover.

The challenge

A ransomware attack on a large local government entity affected several departments and disrupted critical communications and IT systems.

The LevelBlue Managed Detection and Response (MDR) SOC team noticed alerts indicating a potential ransomware attack. The team created an investigation within LevelBlue USM Anywhere, an open XDR platform that received alerts from the PsExec utility tool used within the customer's environment. This tool allows users to remotely execute, and threat actors are known to abuse it to remotely execute commands or deploy malware and move laterally through an environment.

The solution

The SOC team conducted an in-depth review of log data from 90 days prior to the incident, performed opensource intelligence (OSINT) research, and observed encrypted file extensions that were being uploaded to OneDrive. From this work, LevelBlue analysts determined the attackers were members of the Royal Ransomware Group, known to be responsible for several high-visibility attacks since the end of 2022[1].

The incident was immediately escalated to a LevelBlue incident response (IR) team. The team determined that the attackers had compromised an on-premises, external-facing Microsoft Exchange server running on a Windows Server that was past end-of-life (EOL) support. The attackers were using the server as their beachhead to perform reconnaissance and move laterally across the network before deploying encryption malware.

The IR team also established when the server was most likely compromised through the USM Anywhere platform's integration with ExtraHop, a third-party anomaly detection tool. The tool had detected large amounts of data being exfiltrated from multiple Windows assets to an IP address known to be a Cobalt Strike command-and-control server using a technique known as SSH tunneling. While Cobalt Strike is a legitimate penetration testing product, it is also used by threat actors to compromise networks.

The compromised server was observed using various known attacker tactics, techniques, and procedures (TTPs) to identify information sources and systems of interest and to perform suspicious and malicious actions in the customer's environment.

The result

LevelBlue analysts served as vital first responders during the incident, quickly communicating the issue to the municipality and helping them accelerate their time to respond by providing recommendations on how to quarantine the attack and contain the damage.

LevelBlue analysts stayed in close communication with the client at the height of the attack, providing 24×7 support. As the municipality shared updates on which of its servers and services were impacted, the analysts gave detailed guidance on containment and remediation. This allowed the client to act quickly to contain the numerous affected hosts, reset the credentials for several accounts that were observed to have been used by attackers, and rebuild critical servers.

Within 24 hours of initial contact, the LevelBlue team had issued the client a detailed report on the incident findings and provided recommendations to help protect against future ransomware attacks. The team also recommended actions to take for legal and compliance reasons and in the event that deeper post-incident forensic review is needed.

The municipality was also using LevelBlue's managed firewall services. This permitted the LevelBlue SOC team to provide multiple indicators of compromise (IOCs) including IP addresses and domains, which the LevelBlue Managed Firewall team blocked at the beginning of the investigation.

The customer was advised to continue working closely with the LevelBlue Managed Firewall team to review network firewall rules to prevent an attacker's lateral movement for internal only (i.e., "East/West") traffic and for external and internal (i.e., "North/South") traffic.

To protect against future attacks, LevelBlue analysts advised the client to:

- Replace EOL assets and software
- Routinely check assets for secure configurations
- Properly patch known vulnerabilities
- Use application whitelisting to prevent unknown applications from being executed in the environment
- Allow only known and approved remote access and management tools to be installed and executed

Because the attackers had compromised a domain controller, analysts also recommended that the client reset user credentials across the environment and closely monitor the environment for future findings. Additionally, since the attackers had access to the client environment for a significant amount of time, LevelBlue analysts advised against restoring from recent backups and recommended instead rebuilding compromised or encrypted servers.

During the incident, LevelBlue analysts identified four new anomalous events. The LevelBlue SpiderLabs threat intelligence team, which works in close collaboration with the LevelBlue SOC, has used these findings to develop four new, high-fidelity correlation rules that will generate alarms for similar anomalous activity across the LevelBlue managed detection and response customer base.

These rules were subsequently deployed to the municipality's environment. Not only will they help protect the customer's fleet from similar attacks, but they will also help protect other LevelBlue clients using the LevelBlue USM Anywhere platform.

1 https://www.securityweek.com/organizations-warned-of-royal-ransomware-attacks/